

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-266465

(43)Date of publication of application : 31.10.1990

(51)Int.Cl.

G06F 15/30

G09C 1/00

(21)Application number : 01-087272

(71)Applicant : NIPPON TELEGR & TELEPH
CORP <NTT>

(22)Date of filing : 05.04.1989

(72)Inventor : OKAMOTO TATSUAKI
OTA KAZUO

(54) CERTIFICATION SYSTEM

(57)Abstract:

PURPOSE: To attain rapid and untraceable certification by allowing a person to be inspected to secrete a random number component in a system constituted of a certifier, the inspected person and an inspector.

CONSTITUTION: The person B to be inspected applies the corresponding relation of an inquiry message and that of an answer message as secret random numbers, and when the values are secreted, the corresponding relation of data communicated between the certifier A and the inspected person B and between the inspected person B and the inspector C can be hidden. Namely, the fact that the A guarantees the B's identity can be certified to the C without clearing the B's identity in user's certification processing. In message certification

processing, the B allows the A to sign without informing the contents of a message (m). Even if the A and the C conspire with each other, B's identity is not revealed and the transmission of the message (m) from the B can not be also detected. Consequently, untraceable certification processing can be rapidly attained.

